UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE NEW YORK TIMES COMPANY, NICHOLAS CONFESSORE, and GABRIEL DANCE, Plaintiffs, -v- FEDERAL COMMUNICATIONS COMMISSION, Defendant.	18 Civ. 8607 (LGS)

DEFENDANT FEDERAL COMMUNICATIONS COMMISSION'S REPLY MEMORANDUM OF LAW IN FURTHER SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT AND IN OPPOSITION TO PLAINTIFFS' CROSS-MOTION FOR SUMMARY JUDGMENT

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel.: (212) 637-2721
Fax: (212) 637-2686
Email: tomoko.onozawa@usdoj.gov

TOMOKO ONOZAWA
Assistant United States Attorney, *Of Counsel*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Defendant Federal Communications Commission ("FCC"), by its attorney, Geoffrey S. Berman, United States Attorney for the Southern District of New York, respectfully submits this reply memorandum of law in further support of its motion for summary judgment and in opposition to the cross-motion of plaintiffs The New York Times Company, Nicholas Confessore, and Gabriel Dance's ("Plaintiffs") for summary judgment.

ARGUMENT

A. The IP Addresses and User-Agent Headers Sought by Plaintiffs Are Exempt From Disclosure Under FOIA Exemption 6

The common thread running through Plaintiffs' original and multiple revisions of their FOIA Request is their misguided insistence that the FCC must disclose the IP addresses and User-Agent headers of all comments publicly posted to the FCC's *Restoring Internet Freedom* rulemaking proceeding ("Docket No. 17-108") through its Electronic Comment Filing System ("ECFS"). The IP Addresses and User-Agent headers sought by Plaintiffs' latest iteration of its FOIA request, *see* Mem. of Law in Opp. to Def.'s Mot. For Summ. J. and in Support of Pls.' Cross-Mot. For Summ. J. ("Pls.' Opp. Br.") [Dkt. No. 28], at 8 n.7, are exempt from disclosure under FOIA Exemption 6, because the disclosure implicates a personal privacy interest which has not been overridden by a compelling public interest in disclosure.

Plaintiffs contend that "releasing IP addresses and User-Agent headers does not threaten the anonymity of commenters because commenters are not anonymous to begin with." Pls.' Opp. Br. at 11. This entirely misses the mark. The FCC is not seeking to protect "the anonymity of commenters," because commenters are *required* to include a name and a postal address before posting a comment, and every comment, name and postal address submitted to ECFS is accessible to the public. *See* Declaration of Erik Scheibert, dated Mar. 14, 2019 ("Scheibert Decl.") [Dkt. No. 24] ¶¶ 8, 29; *see also* https://www.fcc.gov/ecfs/filings. Nor is the FCC arguing

that an IP address, which is a string of numbers, *see* Scheibert Decl. ¶ 35, and a User-Agent header, which contains specific information about a user's computer system, *id.* ¶ 27, standing alone, can identify an individual user. The point is that, if the FCC is compelled to disclose an individual's IP address, operating system and version, browser platform and version, and language settings, and that information is linked to the individual's publicly-available name and postal address, that disclosure would result in clearly unwarranted invasions of personal privacy, and thus Exemption 6 applies. *Wood v. FBI*, 432 F.3d 78, 86 (2d Cir. 2005).

Plaintiffs claim that the FCC "dramatically overstates" the harm arising out of the improper disclosure of IP addresses and User-Agent headers, and they assert that "most individuals" (but notably not *all*) connect to the Internet using "dynamic IP addressing," whereby an Internet service provider can change a user's IP address. Pls.' Opp. Br. at 12–13. But the fact that an IP address can change at some point in time does not eliminate the risk of harm of disclosure for every commenter to Docket No. 17-108. As Plaintiffs concede and at least one Circuit court recognized, "not all IP addresses are dynamic," *Klimas v. Comcast Cable Commc'ns, Inc.*, 465 F.3d 271, 275 (6th Cir. 2006). Some Internet users, including individual retail customers, can pay to have a static address from their ISP to host their own Internet services such as e-mail, web servers, or web-based cameras. Second Declaration of Erik Scheibert, dated May 2, 2019 ("Second Scheibert Decl.") ¶ 3. Additionally, for those users with dynamic IP addresses, those addresses may remain unchanged for some time, *see id.* ¶ 4, often for months.[1] While most users with dynamic IP addresses who submitted comments to ECFS in

[1] *See also* Jonathan Weinberg, *Hardware-Based ID, Rights Management, and Trusted Systems*, 52 STAN. L. REV. 1251, 1260 n.24 (2000) (a client with a dynamic IP address "could use the same address for months at a time"); Dana Bojcic, "How Often Do IP Addresses Change? (Example)," VICI MEDIA BLOG, http://vicimediainc.com/often-ip-addresses-change (last visited May 2, 2019) (explaining company's finding that the average household in its marketing

2017 will likely have different IP addresses today, it is far from certain that all those users obtained new addresses. *Id.*

Although Plaintiffs assert that disclosing every commenter's IP address and User-Agent heading is appropriate because "an internet-connected device's IP address today may not be its IP address tomorrow," Pls.' Opp. Br. at 12–13, or because the server logs may include the IP addresses of organizations and entities (whose personal information is not subject to the same protection as individuals under Exemption 6), the FCC cannot identify and segregate outdated individual IP addresses and organizational IP addresses from still-existing individual IP addresses. *See* Second Scheibert Decl. ¶ 6. Moreover, as described at length in the agency's opening *Vaughn* declaration, anyone who can link an individual commenter's name and postal address with his or her IP address and User-Agent header can commercially exploit the user's personal information for financial gain, commit identity theft, or otherwise harm the user. *See* Scheibert Decl. ¶¶ 36, 37; Second Scheibert Decl. ¶ 5. These potential harms are widely known[2]

---

campaigns has the same dynamic IP address for nine months); *United States v. Kearney*, 672 F.3d 81, 89 (1st Cir. 2012) (summarizing computer forensics expert affidavit stating that some ISPs change dynamic addresses frequently, "while others may not change dynamic addresses for months or even years").

[2] *See, e.g.*, Digital Marketing Group, "What is IP Targeting and how to use it to build a successful brand," https://thinkdmg.com/what-is-ip-targeting-and-how-to-use-it-to-build-a-successful-brand/ (last visited May 2, 2019) (touting the benefits of "IP targeting," described as "the ability to show ads to specific addresses, office buildings, and even suite numbers" by using "the names, addresses, and zip codes" of advertising targets and running that information through "an IP mapping system where the IP addresses are matched with physical addresses"); Kalev Leetaru, "What Does It Mean for Social Media Platforms to 'Sell' Our Data," FORBES (Dec. 15, 2018), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/#6998d822d6c4 (describing how "data brokers" can link a user's IP address to the address information that users enter into other sites across the web); Andy Greenberg, "Google Can Now Tell You're Not a Robot With Just One Click," WIRED (Dec. 3, 2014), https://www.wired.com/2014/12/google-one-click-recaptcha/ (describing how Google can establish a person's identity by matching an IP address to information the company has already collected about the individual).

and are far from "fanciful and speculative arguments about how the information might be misused." Pls.' Opp. Br. at 2.

Plaintiffs cite *Dep't of the Air Force v. Rose*, 425 U.S. 352 (1976) and *American Civil Liberties Union v. Dep't of Defense* ("*ACLU*"), 543 F.3d 59 (2d Cir. 2008), for the proposition that the agency cannot rely on a "remote and speculative" harm from disclosure. *See* Pls.' Opp. at 13–14. *Rose* and *ACLU* are distinguishable because the records at issue had been redacted for all personal identifying information, and the courts disagreed with the Government's arguments that the requesters would still be able to identify the individuals from other contexts. In *Rose*, the Army refused to disclose entire Air Force Academy case summaries of honors and ethics hearings, even though it had already deleted personal references and other identifying information in the summaries. 425 U.S. at 355, 380. The Supreme Court held that the summaries had to be disclosed because the agency's redactions already addressed Exemption 6's individual confidentiality concerns. *Id.* at 380–81. In *ACLU*, this Court ordered the release of Army photographs showing the abusive treatment of detainees by United States soldiers in Iraq and Afghanistan, with redactions for "all identifying characteristics of the persons" depicted in them. 543 F.3d at 64–65. However, the Government argued on appeal that the redacted photos still constituted an unwarranted invasion of personal privacy, because when "combined with information contained in the investigative reports associated with the detained images," it was possible for the public to identify the detainees in the photos. *Id*. at 84. The Second Circuit disagreed, and held that the redactions already eliminated any "cognizable privacy interest at issue." *Id.* at 86. Here, by contrast, the names and postal addresses of commenters to Docket No. 17-108 are publicly available, but when matched to the IP addresses and User-Agent

headings (which are not available, and are thus sought by Plaintiffs) will lead to a clearly unwarranted invasion of their personal privacy.

Plaintiffs also mischaracterize the warning on ECFS which informs all commenters that "You are filing a document into an official FCC proceeding. All information submitted, including names and addresses, will be publicly available via the web." *See* Scheibert Decl. ¶ 8; https://www.fcc.gov/ecfs/filings. The only information that a commenter can voluntarily and knowingly enter on ECFS is the commenter's name, postal address, and the comment itself. *Id.*; *see also* Second Scheibert Decl. ¶ 2. By contrast, log data, including the IP address of the commenter's device and the User-Agent heading, is automatically recorded in the server log as part of the technical interaction between the user's computer and ECFS. *Id*. Users cannot voluntarily "submit" their IP address and User-Agent information by typing them into a field and hitting "send." *Id.* Plaintiffs wrongly assume that "commenters are on notice that the most revealing of personal information will be made public and that the information to be made public exceeds just name and address," Pls.' Opp. Br. at 15, when in reality, many users are likely unaware that their computer is automatically transmitting their IP address and User-Agent information to ECFS. *Id*.

Contrary to Plaintiffs' contention, *People for the Am. Way Found. v. Nat'l Park Serv.*, 503 F. Supp. 2d 284 (D.D.C. 2007) and *Alliance for the Wild Rockies v. Dep't of the Interior*, 53 F. Supp. 2d 32 (D.D.C. 1999) do not support Plaintiffs' position that Exemption 6 mandates the disclosure of an individual commenter's IP address and User-Agent heading. *See* Pls.' Opp. Br. at 10. Neither case involved IP addresses or User-Agent headings. In *People for the American Way*, the Government invoked Exemption 6 to withhold the names, home addresses, telephone numbers, and personal e-mail addresses of individuals who submitted unsolicited e-mail

comments to the agency regarding a proposed change of video on display at the Lincoln Memorial. 503 F. Supp. 2d at 305. The district court decided that only the *names* of the commenters could be disclosed, but not their addresses and phone numbers, finding that "it is unclear what the public would learn about agency conduct by the disclosure of personal addresses and phone numbers." *Id.* at 307. In *Alliance for Wild Rockies*, plaintiffs sought to compel two federal agencies to disclose the names and addresses of individuals who submitted written comments to defendants' proposed rulemaking. 53 F. Supp. 2d at 33. The district court held that the commenters' names and addresses should be disclosed because of the public interest in full disclosure of written comments received by the agencies, *id.* at 36, and noted that the notice of public rulemaking itself stated that "[t]he complete file for this proposed rule," which included the comments submitted, were publicly available. *Id.* at 34. Both cases involved information—names and addresses—which were voluntarily submitted by commenters. Here, by comparison, an individual commenter has no control over the transmission of an IP address and information about the computer system he or she is using.

Plaintiffs also argue that the requested disclosure would shed light on the FCC's purported "principal statutory obligations to ensure that it not allow public participation in the policy-making process to be overrun by bots and fake Russian-originated comments." Pls.' Opp. Br. at 16. Plaintiffs cite no authority for this purported obligation, and indeed the relevant statute emphasizes inclusion rather than exclusion.[3] In any case, Plaintiffs fail to show the "necessary nexus between the requested information and the asserted public interest that would be advanced by disclosure" of the IP addresses and User-Agent headings of *bona fide* commenters to Docket

[3] As Plaintiffs acknowledge, *see* Pls.' Opp. Br. at 17, the Administrative Procedure Act requires agencies to give "interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments," and to undertake a "consideration of the relevant matter presented" when engaging in rule making. 5 U.S.C. § 553(c).

No. 17-108, in addition to those of purported "bots and fake Russian-originated comments." *See Nat'l Archives and Records Admin. v. Favish*, 541 U.S. 157, 172–73 (2004). Indeed, Plaintiffs' asserted interest cannot override the privacy interests of individuals who were not of alleged fake Russian origin or automated bots who posted substantive comments to Docket No. 17-108.

Plaintiffs also assert that revealing the IP addresses and User-Agent headers of everyone who submitted comments to Docket No. 17-108 will reveal "who corrupted the notice-and-comment process, and how they did it," Pls.' Opp. Br. at 16, but fail to explain how learning the identity and location of "cloud-based automated bots" will further the public's understanding of the *agency's* notice and comment process. *U.S. Dep't of Defense v. Fed. Labor Relations Authority,* 510 U.S. 487, 495 (1994). *See also U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 774 (1989) (upholding withholding of criminal rap sheet of individual who allegedly had improper dealings with Congressional representative because disclosure would "tell us nothing directly about the character of the *Congressman's* behavior") (emphasis in original); *Gannett Satellite Info. Network, Inc. v. U.S. Dep't of Educ.*, Civ. A. No. 90-1392, 1990 WL 251480, at *6 (D.D.C. Dec. 21, 1990) (plaintiff's demand for names, addresses and social security numbers of individuals defaulting on student loans "does not explain how the student loan program is administered, but, rather, is an inquiry into personal information concerning the person to whom the files are related"). If there is any question about what the FCC relied upon when it issued its final rule in Docket No. 17-108, the agency's declaratory ruling and report on the final rule,[4] which runs over 500 pages, describes all of the public comments and other sources which the agency considered.

[4] *See* FCC Declaratory Ruling, Report and Order, and Order, WC Docket No. 17-108 (Dec. 14, 2017), 33 FCC Rcd. 311, *available at* 2018 WL 305638.

Plaintiffs cite *Prechtel v. Fed. Commc'ns Comm'n*, 330 F. Supp. 3d 320 (D.D.C. 2018) for the proposition that there is an overriding public interest in releasing the IP addresses and User-Agent headings of all commenters to Docket No. 17-108. *See* Pls.' Opp. Br. at 16–17. *Prechtel*, however, is distinguishable in multiple material respects. In that case, the district court granted plaintiff's request for the e-mail addresses of "bulk comment submitters" to Docket No. 17-108—*i.e.,* the e-mail address of the individual who uploaded to ECFS a spreadsheet containing multiple individual comments, a process which enabled organizations to collect its members' comments and submit them at once. *Id.* at 324. In so doing, the district court held that "[t]he bulk submitters' privacy interest in their email addresses is minimal in this context," because "[t]he email addresses of those intending to influence the Commission's decision-making were subject to public disclosure." *Id.* at 329. By comparison, the IP addresses and User-Agent headings sought here would constitute a "clearly unwarranted invasion of personal privacy." *See supra* at 3. Moreover, in *Prechtel*, the district court noted that the "[r]elative public value" of the bulk submitters' e-mail addresses "might have been a slightly closer call had the Commission not already released over twenty million e-mail addresses." *Id.* at 331–32. Here, the FCC has never made public the IP addresses and User-Agent headings of any commenter to ECFS.

B. FOIA Does Not Require The FCC to Research and Develop a New Way to Limit Server Log Data to Comments From Docket No. 17-108

As set forth in the FCC's opening brief and *Vaughn* Declaration, segregating comments to Docket No. 17-108 from the raw data in the API proxy server logs is nothing like performing an electronic database search as contemplated by FOIA. Scheibert Decl. ¶¶ 17, 30. The issue is not whether FCC must undertake an "unreasonably burdensome" search for responsive records, as Plaintiffs contend. *See* Pls.' Opp. Br. at 20–21. Rather, the question is whether FOIA

requires the FCC in the first instance to conduct research, as opposed to performing a search, by designing, programming, and testing a new computer script solely to extract the server log data in a way that satisfies Plaintiffs' FOIA Request. "[T]he FOIA imposes no duty on the agency to create records," and "also does not require agencies to conduct research by 'answer[ing] questions disguised as a FOIA request.'" *Nat'l Security Counselors v. Central Intelligence Agency*, 898 F. Supp. 2d 233, 269 (D.D.C. 2012) (citations omitted, alterations in original).

The FCC acknowledges that "if the agency already stores records in an electronic database, searching that database does not involve the creation of a new record. Likewise, sorting a pre-existing database of information to make information intelligible does not involve the creation of a new record . . . ." *Id.* at 270. At the same time, courts have recognized a "distinction between searching and either performing research or creating records," and have acknowledged situations where extracting electronic data can "cross[] the all-important line between searching a database, on the one hand, and either creating a record or conducting research in a database on the other." *Id. See also Labella v. FBI*, No. 11-CV-0023, 2012 WL 948567, at *12 n.12 (E.D.N.Y. Mar. 19, 2012) (FOIA did not require agency to respond to request for "aggregate data" related to specific victim class and subgroups, and which included specific classes of other data). The cases cited by Plaintiffs pertain to "database searches." *See, e.g., Schladetsch v. U.S. Dep't of Housing and Urban Dev.*, No. 99-0175, 2000 WL 33372125, at *3 (D.D.C. Apr. 4, 2000) (discussing electronic database searches). But as described at length in the FCC's *Vaughn* Declaration, designing a script to extract information related to Docket No. 17-108 from server logs is nothing like a database search, and crosses over the line to conducting research to answer Plaintiffs' question about which IP addresses can be correlated to Docket No. 17-108. Scheibert Decl. ¶ 30.

Notwithstanding the difficulties of designing a new script to be applied for this specific purpose, Plaintiffs wrongly assert that "the difficulty of this matching would presumably depend on the number and timing of ECFS comments submitting in other FCC proceedings," and assume that the matching would be easy based on their estimation that, for the relevant time frame, only 300 comments were submitted in 46 other FCC proceedings, as compared to nearly 5 million comments posted to Docket No. 17-108 alone. Pls.' Opp. Br. at 21–22. By FCC's calculation, however, over 34,000 comments, not 300 comments, were posted on ECFS during the same timeframe for matters outside of Docket No. 17-108.[5] Moreover, if the Court holds that the FCC is not be required to segregate from the entire API proxy server log only the comments posted to Docket No. 17-108, Plaintiffs demand that "the entire log must still be produced to The Times." Pls.' Opp. Br. at 22. Producing "the entire log" from April 26, 2017 to June 7, 2017, however, would include the IP addresses and User-Agent headers of over 34,000 individuals who posted comments outside of Docket No. 17-108. Because the disclosure of IP addresses and User-Agent headers for those 34,000 comments have no nexus to Plaintiffs' asserted interest in knowing "who corrupted the notice-and-comment process" in Docket No. 17-108, Pls.' Opp. Br. at 16, Plaintiffs' alternative request for the *entire* API proxy server log should be denied.

[5] An ECFS search (https://www.fcc.gov/ecfs/) for all comments received in that date range, with no restriction for proceeding number, yields 5,006,148 results. The same search restricted to Docket No. 17-108 yields 4,971,895 results. The difference between those sums, 34,253, represents the number of comments received that were not filed in Docket No. 17-108. Plaintiffs' calculation may have differed because it was apparently based on a search of 46 other docketed proceedings, *see* Pls.' Opp. Br. at 21, as opposed to all comments received on ECFS, including those in any docket (which may number more than 46) and in non-docketed proceedings. Non-docketed proceedings include matters for which the FCC has not assigned a docket number—for example, a petition asking the FCC to open a brand-new docket and start an entirely new rulemaking proceeding. Users can still make filings in such proceedings through ECFS (https://www.fcc.gov/ecfs/filings/nodocket), but no docket number is required.

CONCLUSION

For the foregoing reasons, the Court should grant summary judgment for the FCC and deny Plaintiffs' cross-motion for summary judgment.

Dated: May 2, 2019
New York, New York

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
Attorney for Defendant Federal Communications Commission

By: */s/ Tomoko Onozawa*
TOMOKO ONOZAWA
Assistant United States Attorney
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel.: (212) 637-2721
Fax: (212) 637-2686
Email: tomoko.onozawa@usdoj.gov